STRATEGI KEAMANAN INFORMASI DALAM MENGHADAPI ANCAMAN SIBER PADA SISTEM PENGADAAN SECARA ELEKTRONIK (STUDI SERANGAN *HACKER* PADA SPSE PROVINSI LAMPUNG TAHUN 2015)

INFORMATION SECURITY STRATEGY TO COUNTER CYBER THREATS IN ELECTRONIC PROCUREMENT SYSTEMS (STUDY OF HACKER ATTACKS IN SPSE PROVINSI LAMPUNG 2015)

Adi Wijaya[1], Suhirwan[2], Rudy AG Gultom[3]

Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan Unhan

(adi.wijaya@idu.ac.id)

Abstrak-- Keamanan Informasi di era perkembangan teknologi saat ini telah menjadi kebutuhan yang wajib di penuhi. Pemerintah sebagai salah satu pemanfaat teknologi telah melahirkan sistem *elektronik procurement* yang merupakan bentuk dari *elektronik goverment*. Beralihnya proses pengadaan ke dalam sistem elektronik justru menimbulkan kerentanan terhadap keamanan sistem informasi tersebut. Hal ini menyebabkan terjadinya serangan *hacker* pada sistem pengadaan secara elektronik (SPSE) Provinsi Lampung tahun 2015 yang mengakibatkan ratusan paket yang sedang proses tander harus tander ulang. Maka dari itu dibutuhkan suatu strategi keamanan informasi yang dapat mencegah terjadinya serangan *hacker* maupun ancaman siber tersebut. Untuk membangun strategi keamanan informasi tersebut menggunakan model keamanan informasi *defense in depth* sebagai teori atau pisau analisis. Pelaksanaan penelitian ini menggunakan metode penelitinan kualitatif dengan pendekatan studi kasus. Hasil penelitian menunjukan bahwa strategi keamanan informasi dalam menghadapi ancaman siber pada sistem pengadaan secara elektronik Provinsi Lampung belum memenuhi aspek-aspek pada model keamanan informasi *defense in depth* yaitu: *governance, people, processes,* dan *technology*.
Kata Kunci: keamanan informasi, ancaman siber, strategi, spse provinsi lampung

***Abstract**-- Information security in the current era of technological development has become a necessity that must be fulfilled. The government as one of the technology users has produced a procurement electronic system which is a form of electronic government. The shifting of the procurement process into an electronic system actually creates vulnerability to the security of the information system. This led to a hacker attack on Lampung's Sistem Pengadaan Secara Elektronik (SPSE) in 2015 which resulted in hundreds of packages being tandered to have to be restarted. Therefore we need an information security strategy that can prevent hacker attacks and cyber threats. To build an information security strategy using the defense in depth information security model as a theory or analysis knife. The implementation of this study used a qualitative research method with a case study approach. The results showed that the information security strategy in dealing with cyber*

[1] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan.
[2] Fakultas Strategi Pertahanan Universitas Pertahanan.
[3] Program Studi Teknologi Penginderaan, Fakultas Teknologi Pertahanan, Universitas Pertahanan.

threats in the electronic procurement system of Lampung Province had not fulfilled aspects of the defense in depth information security model, that are: governance, people, processes, and technology.
Keywords: information security, cyber threat, strategy, spse provinsi lampung

Pendahuluan

Teknologi kini telah menjadi kebutuhan bagi setiap orang, dengan adanya teknologi semua bisa menjadi lebih mudah dan cepat. Perkembangan teknologi saat ini telah memasuki era revolusi industri 4.0, era ini ditandai dengan segala sesuatu yang kini telah berbasis teknologi informasi dan komunikasi dimana internet digunakan sebagai media pertukaran informasi tersebut. Dengan adanya pemanfaatan teknologi informasi dan komunikasi ini segala sesuatu kini bisa diakses dengan mudah melalui internet. Perkembangan teknologi informasi dan komunikasi dengan memanfaatkan teknologi internet kini semakin canggih dan kompleks. Seiring dengan hal tersebut, manusia sebagai pemilik dan pemakai teknologi itu sendiri terus meningkatkan pemanfaat dari teknologi informasi dan komunikasi tersebut agar sesuai dengan apa yang diharapkan. Hasilnya, kini teknologi telah dapat menembus berbagai aspek kehidupan. Pemanfaatan teknologi informasi dan komunikasi sendiri saat ini telah banyak digunakan dalam bidang pendidikan, pertanian, perindustrian, dan juga pemerintahan.

Pemerintah sebagai organisasi yang memiliki kewajiban memberikan pelayanan publik yang merata keseluruh warga negara, harus senantiasa berusaha memperbaiki kualitas pelayanannya. Peningkatan kualitas pelayanan tersebut dapat dilaksanakan dengan menggunakan teknologi informasi yang sesuai dengan kebutuhan organisasi yang mampu mengelola data dengan cepat, efektif dan efisien serta menghasilkan informasi yang tepat, cepat, dan akurat. Untuk mewujudkan pelayanan cepat, tepat, dan sederhana setiap Badan Publik: menunjuk Pejabat pengelola Informasi dan Dokumentasi, dan membuat serta mengembangkan sistem penyediaan layanan informasi secara cepat, mudah, dan wajar sesuai dengan petunjuk teknis standar layanan Informasi Publik yang berlaku secara nasional. [4] Pada sektor pelayanan publik yang dilakukan oleh pemerintah, perkembangan teknologi

[4] Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 13, ayat (1).

informasi dan komunikasi telah melahirkan model pelayanan publik yang dilakukan melalui *e-government*.

Pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan diyakini akan meningkatkan efesiensi, efektifitas, transparansi serta akuntabilitas penyelenggaraan pemerintahaan.[5] Melalui pengembangan *e-government* dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi.

E-government menjadi sangat popular sejalan dengan perkembangan teknologi informasi dan komunikasi. Berbagai Negara dibelahan dunia berlomba mengimplementasikan *e-government* dengan strategi yang disesuaikan dengan kondisi sosial politik serta geografisnya masing-masing, yang tujuan akhirnya diharapkan meningkatkan kualitas kinerja pemerintah terutama dalam lingkup pelayanan masyarakat sehingga dapat bermanfaat bagi segenap warga negaranya. Bahkan di Indonesia khususnya di daerah-daerah yang telah mengimplementasikan *e-government* dengan strategi yang telah direncanakan di daerah tersebut. Dapat dikatakan bahwa *e-government* adalah penyelenggaraan kepemerintahan yang berbasis elektronik. Dengan menerapkan *e-government* diharapkan mutu pelayanan kepada publik dapat lebih ditingkatkan, baik dari segi efisiensi dan efektivitas biaya, maupun dari segi implementasinya yang menjadi lebih mudah dan transparan. Salah satu produk dari *e-government* yang sudah banyak diterapkan di intansi pemerintah ialah *e-procurement* atau pengadaan secara elektronik.

E-procurement adalah proses pengadaan barang/jasa secara online melalui internet, dimana seluruh proses pengumuman, pendaftaran, proses penawaran, *aanwijzing*, hasil evaluasi atas penawaran dilakukan dengan memanfaatkan sarana teknologi informasi.[6] *E-procurement* dapat dilakukan melalui dua cara yang terdiri dari *e-tendering* dan *e-purchasing*. Sebelum adanya konsep *e-procurement*, Pengadaan barang dan jasa masih menggunakan cara manual yaitu dengan mempertemukan langsung pihak-pihak yang terkait seperti penyedia barang dan jasa dengan panitia pengadaan.

[5] Instruksi Presiden Nomor 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government.

[6] Mochammad Jasin, *Mencegah Korupsi Melalui E-procurement,* (Jakarta: Komisi Pemberantasan Korupsi, 2007), hlm. 3.

Proses yang dilakukan secara manual ini memiliki beberapa kelebihan dan kelemahan. Kelebihan yang didapat yaitu para pengguna dan penyedia barang dan jasa dapat mengetahui proses pengadaan yang berlangsung secara bersama-sama. Tetapi kelemahan dari tahap-tahap pelaksanaan pengadaan barang dan jasa konvesional dirasa kurang efektif pada waktu dan biaya.

Dari sudut pandang tersebut, pemerintah akhirnya menentukan langkah positif dengan menerapkan *e-procurement* untuk seluruh instansi pemerintah. Untuk mendukung aktifitas pengadaan barang dan jasa, beberapa instansi pemerintah mendirikan pusat-pusat Layanan Pengadaan Secara Elektronik (LPSE).

Pusat layanan ini mengelola segala sesuatu yang berkaitan dengan proses elektronik dalam pengadaan barang dan jasa pemerintah. Layanan Pengadaan Secara Elektronik (LPSE) diimplementasikan dalam bentuk pengadaan barang dan jasa secara elektronik yang memfasilitasi proses lelang secara elektronik. Aplikasi Sistem Pengadaan Secara Elektronik (SPSE) merupakan aplikasi e-pengadaan yang dikembangkan oleh Lembaga Kebijakan Pengadaan barang atau jasa Pemerintah (LKPP) untuk digunakan oleh instansi seluruh Indonesia.

Namun dengan memanfaatkan teknologi infomasi pada sistem pengadaan barang dan jasa, justru menimbulkan kendala tersendiri. Hal ini disebabkan dengan menggunakan sistem pengadaan secara elektronik yang berbasis teknologi informasi menyebabkan kerentanan terhadap keamanan dari sistem informasi itu sendiri. Sehingga pada pelaksanaanya, sistem *e-procurement* ini kerap kali terganggu oleh berbagai ancaman siber. Salah satu ancaman siber yang kerap kali mengganggu pelaksanaan sistem *e-procurement* ialah serangan *hacker*. Akibat serangan *hacker* tersebut membuat pemenuhan kebutuhan akan layanan publik khususnya pada layanan pengadaan barang/jasa di pemerintah menjadi tidak maksimal. Di Indonesia sendiri banyak sekali terjadi kasus serangan *hacker* yang menyerang sistem pengadaan secara elektronik, beberapa kasus serangan yaitu:

Pada tahun 2015, terjadi peretasan pada Sistem Pengadaan Secara Elektronik (SPSE) provinsi Lampung. Pada tanggal 22 April 2015 SPSE Provinsi Lampung mengalami kerusakan server akibat serangan *hacker*. Dampak dari serang

tersebut membuat 166 dari 168 paket yang sedang proses lelang harus tender ulang.[7] Peretasan-peretasan yang dilakukan oleh para hacker terhadap Sistem Pengadaan Secara Elektronik ini tentu sangat mengganggu jalannya proses pemerintah sehingga program yang harusnya bisa dikerjakan sesuai jadwal menjadi tertunda akibat serangan *hacker* ini. Di tahun yang sama dengan LPSE Provinsi Lampung yaitu tahun 2015, LPSE Kabupaten Mesuji juga mendapat serangan hacker. Akibat ulah *hacker* tersebut menyebabkan website LPSE Kabupaten Mesuji tidak dapat di akses atau di buka sehingga dokumen tidak dapat diunduh. Serangan hacker tersebut juga telah mengganggu sistem yang ada.[8]

Pada tahun 2016, terjadi peretasan yang dilakukan oleh *hacker* dengan modus memanipulasi akses LPSE milik Kementerian PUPR dengan cara menerobos atau menjebol sistem pengamanan dengan melakukan *SQL Injection* ke situs Kementerian PUPR, sehingga terdapat laporan dari beberapa penyedia jasa yang tidak dapat login ke dalam sistem LPSE terkait proses lelang.[9] Selain itu, terjadi juga peretasan terhadap situs LPSE Pemkab Mojokerto di tahun yang sama yaitu tahun 2016, akibat peretasan ini membuat proses lelang secara online lumpuh dan mengakibatkan pihak LPSE Pemkab Mojokerto melakukan tender ulang terhadap proyek-proyek yang gagal tender.[10]

Untuk menghadapi ancaman siber tersebut maka dibutuhkan pula suatu sistem keamanan yang dapat melindungi sistem informasi tersebut. Hal ini dilakukan agar pemanfaatan dari teknologi informasi pada sistem pengadaan secara elektronik dapat lebih maksimal. Keamanan informasi harus memiliki kehandalan yang tinggi agar dapat mengurangi dan meminimalisir resiko atas kerugian yang mungkin timbul, terkait dengan penggunaan teknologi

---

[7] Yulianto, Beni. "Awalnya Diserang Hacker, Katanya Sudah Bisa Diakses, Nyatanya Tak Bisa" Dalam http://lampung.tribunnews.com/2015/05/23/awalnya-diserang-hacker-katanya-sudah-bisa-diakses-nyatanya-tak-bisa diakses pada 28 juli 2018

[8] Alzoni. "Situs Mesuji Kerap Dihacker". Dalam http://le-ut.blogspot.com/2015/08/situs-lpse-mesuji-kerap-dihacker.html diakses pada 4 Agustus 2018.

[9] Putri Kurniawati, "Hacker Pembobol LPSE Kementerian PUPR Terancam Kurungan Empat Tahun Penjara" Dalam https://www.kupastuntas.co/2016/08/hacker-pembobol-lpse-kementerian-pupr-terancam-kurungan-empat-tahun-penjara/ diakses pada 4 Agustus 2018.

[10] Tritus Julan, "Laman LPSE Diretas, Proses Lelang Kacau" Dalam http://koran-sindo.com/page/news/2016-05-10/6/47/Laman_LPSE_Diretas Proses_Lelang_Kacau diakses pada 4 Agustus 2018

informasi. Maka dari hal tersebut diperlukan suatu upaya yang dapat menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik (SPSE) di masa yang akan datang. Guna mewujudkan hal tersebut maka diperlukan sebuah strategi yang dapat mengamankan sistem tersebut. Maka peneliti mengunakan model keamanan informasi *defense in depth* untuk mengamankan sistem dari serangan *hacker* maupun ancaman siber lainnya.

Metodologi Penelitian

Metodologi penelitian pada hakikatnya adalah cara ilmiah guna mendapatkan data untuk maksud dan tujuan serta untuk kegunaan tertentu[11]. Maka agar hal-hal yang ingin dicapai dari sebuah penelitian tersebut dapat terwujud secara ilmiah, diperlukan sebuah kerangka metodologi penelitian yang jelas dan terukur yang di dalamnya dapat memberikan gambaran terkait upaya pencarian dan penggalian data sehingga dapat dipertanggungjawabkan secara ilmiah. Dalam penelitian ini menggunakan model keamanan informasi *defense in depth* sebagai pisau analisis.

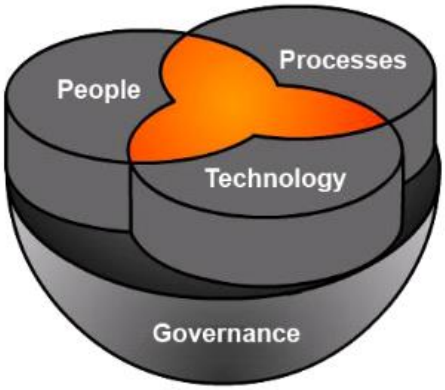
Defense in depth adalah konsep perlindungan jaringan komputer dengan serangkaian mekanisme pertahanan sehingga jika satu mekanisme gagal, yang lain akan ada untuk menggagalkan serangan. Karena ada banyak penyerang potensial dengan berbagai macam metode serangan yang tersedia, dengan memanfaatkan strategi *defense in depth* akan mengurangi risiko karena serangan yang sukses membutuhkan biaya yang sangat mahal.[12]

Prinsip mendasar dalam *defense in depth* adalah pendekatan keseimbangan dan koordinasi antara *people*, *process* (*operation*) dan *technology*[13], sedangkan unsur *governance* bertanggungjawab mengelola koordinasi elemen-elemen ini. Agar *defense in depth* dapat berhasil diimplementasikan dalam strategi organisasi, perencanaan dan struktur harus memasukkan elemen-elemen inti dari *defense in depth* yaitu *governance*, *people*, *process and technology*. Seperti didefinisikan oleh *Australian Government Attorney-General's Department*, sebagai berikut:

[11] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D*, (Bandung: Alfabeta, 2015), hlm.2.

[12] SANS Institute InfoSec Reading Room, *Defense in depth*. (United State: 2001), hlm. 1.

[13] National security Agency, *Defense in dep*th dalam www.nsa.gov/snac/support/defense indepth.pdf diakses pada 4 Agustus 2018.



Gambar 1. Elemen *Defense In Depth*
Sumber : Trusted Information Sharing Network, Australia Tahun 2018

1) *Governance*

Komponen ini mengacu pada kerangka manajemen yang digunakan untuk memberikan pengawasan dan koordinasi *people*, *process* dan *technology*, yang meliputi :

- Manajemen resiko
- Keamanan Informasi
- Kebijakan dan penyesuaian manajemen

2) *People*

Komponen ini menguraikan definisi, pemeliharaan, dan penegakan peran dan tanggung jawab keamanan bagi karyawan dan vendor internal dan eksternal, yaitu :

- Keamanan Personal (termasuk kesadaran pengguna).

3) *Processes*

Komponen ini menggambarkan definisi, pemeliharaan, dan tindakan standar yang digunakan untuk mengembangkan dan memastikan bahwa keamanan tetap pada basisnya, yang meliputi :

- Manajemen akses pengguna
- Manajemen respon
- Manajemen audit

4) *Technology*

Komponen ini menjelaskan teknologi dan solusi produk yang digunakan untuk memungkinkan pencapaian tujuan bisnis secara berkelanjutan, yang meliputi :

- Manajemen komunikasi
- Manajemen infrastruktur
- Manajemen arsitektur jaringan
- Keamanan Aplikasi

Adapun pelaksanaan penelitian ini menggunakan metode kualitatif dengan menggunakan pendekatan metode studi kasus yang merupakan suatu metode eksploratif dan analitis yang sangat cermat dan intensif mengenai keadaan suatu unit (kesatuan)[14], dalam hal ini unit yang dimaksud adalah LPSE Provinsi Lampung. Berikut ini peneliti akan menguraikan kerangka metodologi

[14] Usman Rianse, *Metodologi Penelitian Sosial dan Ekonomi, Teori dan Aplikasi,* (Bandung: Alfabeta, 2009), hlm. 92.

penelitian yang digunakan dalam proses pelaksanaan penelitian.

Teknik pengumpulan data merupakan langkah yang paling strategis dalam sebuah penelitian[15]. Menentukan teknik Pengumpulan data menjadi sangat penting agar peneliti mendapatkan data yang sesuai dengan standar yang ditetapkan. Di samping itu, tujuan utama dari sebuah penelitian adalah untuk mendapatkan data, maka dari awal teknik pengumpulan data harus ditetapkan secara jelas.

Pada penelitian ini, digunakan 4 (empat) teknik pengumpulan data yakni teknik wawancara, observasi, teknik studi dokumentasi dan studi kepustakaan. *Pertama,* teknik wawancara merupakan teknik yang dilakukan untuk mengumpulkan data melalui tanya jawab lisan dengan narasumber yang diperlukan[16]. Narasumber yang diwawancarai adalah kepala bagian LPSE Provinsi Lampung, Kepala Subbagian Pengembangan Sistem Informasi LPSE Provinsi Lampung dan Kepala Subbagian Pengendalian dan Administrasi Pembangunan Provinsi Lampung.

Kedua, teknik observasi digunakan untuk menggali data dari sumber data yang berupa peristiwa, tempat atau lokasi, dan benda, serta rekaman gambar.[17] Observasi ini dilakukan dengan melihat langsung aktivitas, dalam penelitian ini melihat langsung kegiatan di Layanan Pengadaan Secara Elektronik (LPSE) provinsi Lampung.

Ketiga, studi dokumen. Dokumen merupakan catatan peristiwa yang sudah berlalu[18]. Dokumen dapat berbentuk tulisan, gambar maupun karya. Dokumen berupa tulisan seperti catatan harian, sejarah kehidupan, biografi, peraturan dan kebijakan. Dokumen berbentuk gambar misalnya foto, gambar hidup, sketsa dan lain-lain. Dokumen berbentuk karya misalnya karya seni seperti patung, gambar, film dan lain-lain[19]. Dengan demikian, peneliti akan menggunakan dokumen-dokumen yang dimiliki oleh lembaga atau subjek yang akan diteliti yakni dokumen yang ada pada LPSE Provinsi Lampung dan Lembaga Kebijakan Pengadaan Pemerintah (LKPP).

Keempat, studi kepustakaan. Menurut Koentjaraningrat teknik kepustakaan merupakan cara

[15] Sugiyono, *op. cit.,* hlm. 224.
[16] Usman Rianse, *op. cit.,* hlm 219.
[17] Ibid. hlm. 64-65
[18] Sugiyono, *op. cit.,* hlm. 240.
[19] *Ibid.*

pengumpulan data bermacam-macam material yang terdapat di ruang kepustakaan seperti koran, buku-buku, majalah, naskah, dokumen dan sebagainya yang relevan dengan penelitian[20].

Hasil dan Pembahasan

LPSE adalah unit kerja yang dibentuk di seluruh Kementerian/ Lembaga/Satuan Kerja Perangkat Daerah/Institusi Lainnya (K/L/D/I) untuk menyelenggarakan sistem pelayanan pengadaan barang/jasa secara elektronik serta memfasilitasi ULP atau Pejabat Pengadaan dalam melaksanakan pengadaan barang dan jasa secara elektronik.[21]

LPSE Provinsi Lampung merupakan salah satu bagian yang terdapat pada Biro Administrasi Pembangunan yang dibentuk berdasarkan Peraturan Daerah Provinsi Lampung No. 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Lampung. Sebelum adanya peraturan daerah ini status LPSE Provinsi Lampung adalah *ad-hoc* (kepanitian). LPSE Provinsi Lampung terbentuk sejak tahun 2010 dan pada tahun 2011 untuk pertama kalinya melakukan proses pengadaan barang/jasa secara elektronik .

Dalam pelaksanaan Pengadaan Barang/Jasa LPSE Provinsi Lampung menerapkan prinsip-prinsip sebagai berikut:

a. Efisien
b. Efektif
c. Transparan
d. Terbuka
e. Bersaing
f. Adil/tidak diskriminatif, dan
g. Akuntabel

Pengadaan barang secara elektronik dilakukan dengan cara *e-tendering* dan *e-purchasing*. Pengadaan barang/jasa secara elektronik bertujuan untuk :

a. Meningkatkan transparansi dan akuntabilitas
b. Meningkatkan akses pasar dan persaingan usaha yang sehat
c. Memperbaiki tingkat efisiensi proses Pengadaan
d. Mendukung proses *monitoring* dan audit, dan
e. Memenuhi kebutuhan akses informasi yang *real time*

[20] Koentjaraningrat, *Metode-Metode Penelitian Masyarakat*, (Jakarta: Gramedia, 1983). hlm. 420.

[21] Peraturan Presiden Nomor 54 Tahun 2010 tentang Pengadaan Barang/Jasa Pemerintah, Pasal 1, ayat (38).

Fungsi LPSE Provinsi Lampung dalam kegiatan layanan pengadaan secara elektronik meliputi:

a. Pengelolaan seluruh sistem informasi Pengadaan Barang /Jasa dan infrastrukturnya
b. Pelaksanaan registrasi dan verifikasi pengguna seluruh sistem informasi Pengadaan Barang/Jasa
c. Pengembangan sistem informasi yang dibutuhkan oleh pemangku kepentingan.

Serangan Hacker Pada SPSE Provinsi Lampung Tahun 2015

Dari hasil penelitian didapatkan data bahwa pada tahun 2015 memang telah terjadi serangan *hacker* pada SPSE Provinsi Lampung yang menyebabkan 168 dari 169 paket pengadaan yang saat itu sedang proses lelang harus dilakukan tander ulang, hal ini diakibatkan oleh serangan *hacker* dengan teknik *Distributed Denial of Service (DDos)* yang membuat *server* SPSE Provinsi Lampung *down* (tidak dapat diakses). Serangan tersebut terjadi tepatnya pada bulan April tahun 2015. Sebelum *server* SPSE Provinsi Lampung *down* (tidak dapat diakses) terjadi serangan secara besar dan terus-menerus menyerang *server* SPSE Provinsi Lampung yang mengakibatkan *floading* yaitu suatu kondisi dimana terlalu banyak yang mengakses *server* diwaktu yang bersamaan, hal ini menyebabkan *server down* sehingga tidak dapat diakses.

Diduga sebelumnya *hacker* tersebut telah meletakan *file java script* kedalam *server* SPSE Provinsi Lampung. Ketika *file* tersebut diaktifkan maka *file* tersebut seperti halnya sinyal yang memberikan tanda dimana lokasi sasaran untuk dilakukannya serangan secara besar-besaran. Namun sampai sekarang siapa pelaku dan bagaimana pelaku bisa memasukan *file java script* tersebut masih belum diketahui. Akibat serangan tersebut, proses pengadaan secara elektronik di LPSE Provinsi Lampung harus ditunda selama satu bulan yang mengakibatkan 168 dari 169 paket yang saat itu sedang proses lelang terpaksa harus tender ulang satu bulan kemudian. Untuk mengatisipasi serangan serupa terjadi lagi, pihak LPSE Provinsi Lampung mengganti *server* yang lama dengan *server* yang baru. Sehingga membutuhkan waktu yang lama untuk instalasi ulang dan penginputan data ulang. Selain menyebabkan tertundanya pelaksanaan pekerjaan proyek pemerintah Provinsi Lampung juga menyebabkan kerugian secara materil akibat serangan tersebut, hal ini dikarenakan LPSE Provinsi Lampung

harus menganggarkan dana untuk pembelian *server* baru.

Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik Provinsi Lampung

Model keamanan informasi *defense in depth* yang peneliti gunakan dalam merancang strategi keamanan informasi ini merupakan model keamanan informasi yang dikembangkan oleh *IT Security Expert Advisory Group (ITSEAG)* yang merupakan bagian dari *Trusted Information Sharing Network (TISN)* Pemerintah Australia. Pada model *defense in depth* yang dikembangkan oleh *IT Security Expert Advisory Group (ITSEAG)* berfokus pada perlindungan 4 elemen/aspek yaitu *People*, *Process*, *Technology*, dan *Governance*.

1. **Aspek *Governace***

   Pada Aspek ini mengacu pada kerangka manajemen yang digunakan untuk memberikan pengawasan dan koordinasi pada aspek *people, processes* dan *technology* yang meliputi: manajemen resiko, keamanan informasi dan penyesuaian kebijakan. Dari aspek ini diketahui bahwa sebelum keluarnya Peraturan Presiden dan Peraturan LKPP yang baru yaitu Peraturan Presiden No. 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, pihak LPSE Provinsi Lampung memiliki turunan berupa Peraturan Daerah No. 8 Tahun 2016 yang mengatur tentang tata kelola LPSE Provinsi Lampung. Namun setelah keluarnya Peraturan yang baru tersebut saat ini LPSE Provinsi Lampung belum memiliki aturan turunan yang baru. Alasan LPSE Provinsi Lampung belum mengeluarkan regulasi turunan tersebut dikarenakan pihak LPSE Provinsi Lampung menilai bahwa di dalam Peraturan Presiden No. 16 Tahun 2018, sudah mengatur dengan sangat jelas terkait pengadaan barang dan jasa. Sehingga saat ini pihak LPSE Provinsi Lampung hanya berpedoman pada peraturan yang sudah ada tanpa membuat aturan turunan. Sedangkan terkait regulasi yang berupa aturan tertulis atau SOP tentang keamanan informasi dan manajemen resiko belum ada. Saat ini LPSE Provinsi Lampung lebih fokus kepada upaya pencapaian standar yang telah ditetapkan oleh LKPP, yaitu terdapat 17 standar yang harus di penuhi oleh setiap LPSE di Indonesia. Dari 17 standar tersebut, LPSE Provinsi Lampung sudah mendapatkan 12 sertifikat terkait

standar pengelolaan LPSE yaitu sertifikat untuk standar: 1. Pengelolaan Layanan Helpdesk, 2. Pengelolaan Kelangsungan Layanan, 3. Pengelolaan Pendukung Layanan, 4. Pengelolaan Resiko Layanan, 5. Pengorganisasian Layanan, 6. Kebijakan Layanan, 7. Pengelolaan Anggaran Layanan, 8. Pengelolaan Aset Layanan, 9. Pengelolaan Hubungan Dengan Layanan, 10. Pengelolaan Kapasitas, 11. Pengelolaan Perubahan, 12. Pengelolaan Sumber Daya Manusia. Sedangkan 5 standar yang belum dicapai yaitu standar : 1. Pengelolaan Keamanan Perangkat, 2. Keamanan Operational Layanan, 3. Keamanan Server dan Jaringan, 4. Pengelolaan Kepatuhan, 5. Penilaian Internal.

Namun yang disayangkan dari 12 pencapaian standar yang sudah di raih LPSE Provinsi Lampung belum ada yang terkait dengan pengelolaan keamanan informasi. Justru 3 standar tentang keamanan informasi yaitu: 1. Pengelolaan Keamanan Perangkat, 2. Keamanan Operational Layanan, 3. Keamanan Server belum tercapai.

Dari apa yang telah diuraikan diatas dapat disimpulkan bahwa pada aspek Governance ini LPSE Provinsi Lampung belum memenuhi standar model keamanan defense in depth hal ini dikarenakan LPSE Provinsi Lampung belum memiliki aturan atau standar terkait pengelolaan keamanan informasi dan manajemen resiko.

2. Aspek *People*

Pada aspek people menguraikan definisi tentang pemeliharaan dan penegakan peran dan tanggung jawab keamanan bagi pegawai dan vendor internal dan eksternal yaitu keamanan personil (termasuk kesadaran pengguna). Saat ini LPSE Provinsi Lampung belum memiliki sumber daya manusia yang cukup khususnya yang dapat memahami *IT,* saat ini LPSE Provinsi Lampung hanya memiliki satu orang pegawai lulusan sarjana komputer. Sehingga hal tersebut masih belum cukup. Terkait kerahasian data dan login, setiap pegawai yang berada di LPSE Provinsi Lampung diikat secara hukum dengan pakta integritas. Sedangkan terkait pembekalan pengetahuan dan kemampuan dalam hal keamanan informasi saat ini LPSE Provinsi Lampung belum pernah mengadakan pelatihan khusus keamanan informasi kepada pengguna SPSE termasuk personil LPSE Provinsi Lampung. Sejauh ini pelatihan hanya berupa pelatihan penggunaan SPSE.

Dari apa yang telah diuraikan terkait aspek *people,* LPSE Provinsi Lampung belum memenuhi aspek *people*. Walaupun dalam hal keamanan personil atau pengguna LPSE Provinsi Lampung telah menggunakan pakta integritas untuk mengikat secara hukum pegawai LPSE, akan tetapi pada hal pengetahuan dan kemampuan tetang keamanan informasi pengguna/personil LPSE Provinsi Lampung belum pernah ada pembekalan dalam bentuk pelatihan. Dan sosialisasi terkait kesadaran pengguna juga belum maksimal karena hanya sebatas pada disampaikan pada sela-sela pelatihan penggunaan aplikasi SPSE.

3. **Aspek *Processes***

Pada aspek *processes* menguraikan tentang bagaimana pemeliharaan dan tindakan standar yang digunakan untuk mengembangkan dan memastikan bahwa keamanan tetap pada basisnya, yang meliputi: manajemen akses pengguna, manajemen respon, dan manajemen audit. Saat ini LPSE Provinsi Lampung belum memiliki SOP terkait manajemen respon, selama ini penanganan permasalahan yang muncul harus berdasarkan keputusan pimpinan. Sehingga belum ada standar baku tentang bagaimana menangani permasalahan. Kemudian terkait manajemen audit, LPSE Provinsi Lampung belum memiliki tim audit internal. Audit yang selama ini hanya dilakukan oleh LKPP selaku pemangku kebijakan. Namun pada sisi manajemen akses pengguna sistem SPSE sendiri sudah menerapkan hal tersebut, hal ini dilakukan dengan membuat level hak akses pengguna. Dengan adanya sistem ini masing-masing pengguna hanya dapat mengakses sesuai dengan tugas dan tanggung jawabnya.

Berdasarkan uraian tersebut dapat disimpulkan bahwa pada aspek processes ini LPSE Provinsi Lampung belum memenuhi standar yang ada. Walaupun pada aspek manajemen akses pengguna sudah memenuhi, namun pada aspek manajemen audit dan manajemen respon belum memenuhi.

4. **Aspek *Technology***

Pada aspek ini menjelaskan tentang teknologi dan solusi produk yang digunakan untuk memungkinkan pencapaian tujuan secara berkelanjutan yang meliputi: manajeman komunikasi, manajemen infrastruktur, manajemen arsitektur jaringan dan keamanan apilkasi.

Berdasarkan pengamatan langsung yang dilakukan oleh peneliti manajemen infrastruktur yang ada, peneliti melihat bahwa dalam hal pengamanan fisik pada server LPSE Provinsi Lampung belum dilakukan. Terlihat bahwa siapapun bisa keluar masuk ruang *server* tanpa pengamanan. Sedangkan untuk artsitektur jaringan internet LPSE provinsi lampung menggunakan jasa layanan PT. Telkom. Kemudian pada sisi manajemen komunikasi, LPSE Provinsi Lampung belum membuat suatu standar atau tata kelola terkait manajemen komunikasi. di ketahui bahwa saat ini pihak LPSE Provinsi Lampung sudah menerapkan beberapa teknik pengamanan aplikasi diantaranya dengan menggunakan *server backup* untuk mengantisipasi jika terjadi serangan terhadap server utama sehingga bisa digantikan dengan *server backup,* selain itu pengamanan aplikasi juga menggunakan *firewall yang* berfungsi sebagai pembatas dan pelindung dari akses-akses yang tidak resmi, selain itu penggunaan *VPN* juga merupakan langkah yang dilakukan oleh LPSE Provinsi Lampung untuk membatasi pengguna yang dapat mengakses secara langsung pada server.

Berdasarkan hasil penelitian tersebut maka dapat disimpulkan bahwa pada aspek *Technology* ini LPSE Provinsi Lampung belum memenuhi standar yang ada pada *defense in depth*. Hal ini dikarenakan LPSE Provinsi Lampung belum menerapkan manajemen komunikasi dan manajamen infrastruktur. Walaupun pada aspek manajemen arsitektur jaringan dan keamanan aplikasi sudah memenuhi.

Kesimpulan

Dalam strategi keamanan informasi dengan menggunakan model keamanan informasi *defense in depth* yang dikembangkan oleh *IT Security Expert Advisory Group (ITSEAG)* di LPSE Provinsi Lampung guna menghadapi ancaman siber pada sistem pengadaan secara elektronik berdasarkan 4 aspek yaitu *People*, *Process*, *Technology*, dan *Governance*. Dihasilkan bahwa:

1. Aspek *Governance*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan LPSE Provinsi Lampung belum memiliki aturan atau standar terkait pengelolaan keamanan informasi dan manajemen resiko.

2. Aspek *People*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan belum adanya kesadaran dan kapasitas terhadap keamanan informasi bagi pengguna/personil.
3. Aspek *Processes*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan masih lemahnya manajemen audit dan belum adanya manajemen respon terhadap suatu *trouble*.
4. Aspek *Technology*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan LPSE Provinsi Lampung belum menerapkan manajemen komunikasi dan manajamen infrastruktur khususnya pengamanan fisik ruang server.

Daftar Pustaka

Alzoni. 2015. *Situs Mesuji Kerap Dihacker*. dalam http://le-ut.blogspot.com/2015/ 08/situs-lpse-mesuji-kerap-dihacker.

Instruksi Presiden No 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government.

Jasin, Mochammad. 2007. *Mencegah Korupsi Melalui E-procurement.* Jakarta: Komisi Pemberantasan Korupsi.

Julan, Tritus. 2016. *Laman LPSE Diretas, Proses Lelang Kacau.* dalam http://koran-sindo.com/page/news/ 2016-05-10/6/47/Laman_LPSE_Diretas_ Proses_Lelang_Kacau

Koentjaraningrat. 1983. *Metode-Metode Penelitian Masyarakat*. Jakarta: Gramedia.

Kurniawati, Putri. 2016. *Hacker Pembobol LPSE Kementerian PUPR Terancam Kurungan Empat Tahun Penjara*. dalam https://www.kupastuntas.co/2016/08/hacker-pembobol-lpse-kementerian-pupr-terancam-kurungan-empat-tahun-penjara/

Peraturan Presiden Nomor 54 Tahun 2010 tentang Pengadaan Barang/Jasa Pemerintah

Rianse, Usman. 2009. *Metodologi Penelitian Sosial dan Ekonomi, Teori dan Aplikasi*. Bandung: Alfabeta.

SANS Institute InfoSec Reading Room. 2001. *Defense in depth*. United State:

Sugiyono. 2015. *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: Alfabeta.

Undang-Undang Republik Indonesia Nomor 14 tahun 2008, Bab IV Pasal 13 ayat 1 huruf a,

Yulianto, Beni. 2018. *Awalnya Diserang Hacker, Katanya Sudah Bisa Diakses, Nyatanya Tak Bisa*. Dalam http://lampung.tribunnews.com/2015/05/23/awalnya-diserang-hacker-katanya-sudah-bisa-diakses-nyatanya-tak-bisa